E-commerce

January 2005

Essential Practices for Information Technology Examination Manual
IT Section

FCA Essential Practices for Information Technology

Based on Industry Standards and FFIEC Examination Guidance

Table of Contents

Page

E-commerce

E-commerce

Introduction:
The financial services industry's use of electronic commerce (E-commerce) to promote their services, disperse information, take online applications, and assist in their own internal operations has increased substantially. Because technology has tended to change rapidly, the array of services and products offered will most likely expand, thereby offering additional income opportunities for Farm Credit System (FCS or System) institutions. While these activities may provide new business opportunities, they will also create new business risks and challenges that must be managed actively. Institution boards of directors and management must understand the risks associated with E-commerce if they are to make informed decisions regarding the development of a particular product or service. An institution may be conducting these services either in-house or through a vendor relationship with other firms, or may be providing such services to other institutions. Regardless of the method used, the institution's board is responsible for ensuring that it understands the related business risks, implements the necessary internal controls, and complies with applicable regulatory requirements.

Examination Objective:
Determine if the board and management have established and maintained effective controls over E-commerce activities. This is accomplished through the following examination objectives:

- **Board and Management Oversight** – Determine the adequacy of board and management oversight of E-commerce activities with respect to policies and procedures, planning, management reporting, and audit.
- **Internal Controls** – Determine if the institution has implemented appropriate controls to ensure the availability and integrity of processes supporting E-commerce services.
- **Legal and Regulatory Compliance** – Assess board and management's understanding of and adherence to legal and regulatory compliance requirements associated with E-commerce activities.

Examination Procedures:
Examination scope should be based on the level of E-commerce activity. The examination should begin with a review of audit activities and a risk assessment for E-commerce. At a minimum, the ***Essential Practices*** for E-commerce should be clearly documented and functioning within the internal control environment. More in-depth examination procedures (such as those found in the *FFIEC E-Banking Booklet*) should be evaluated and incorporated into the examination scope as an institution's size, risk, and complexity increases.

E-commerce

Element	Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
E-commerce Policy			
	Adopt E-commerce policies and procedures to ensure safety and soundness and compliance with laws and regulations. Among other concerns, the policies and procedures must address, when applicable: • **Security and integrity of System institution and borrower data;** • **Privacy of web site customers and visitors;** • **Notices of web site customers or visitors when linking to an affiliate or third party web site;** • **Capability of vendor or application providers;** • **Business resumption after disruption;** • **Fraud and money laundering;** • **Intrusion detection and management;** • **Liability insurance; and** • **Prompt reporting of known or suspected criminal violations associated with E-commerce to law enforcement authorities and FCA under FCA Regulations Part 612 Subpart B.** ***Reason:*** *Establishing applicable policies and procedures is required to comply with laws and regulations, and also contributes to appropriate internal controls for ensuring safety and soundness.*	FCA Regulation 609.930.	E-Banking Booklet (Aug. 2003) pp. 13, 19-20.
E-commerce Business Planning			
	Describe in the institution's business plan the existing and planned E-commerce initiatives, including intended objectives, business risks, security issues, relevant markets, and legal compliance. ***Reason:*** *Placing this information in the business plan is required to comply with regulations. It will also aid the board and management in appropriately preparing for future activities and major investments to provide quality, cost-effective initiatives.*	FCA Regulation 609.935.	E-Banking Booklet (Aug. 2003) pp. 20-21.
E-commerce Controls			
	When applicable, internal systems and controls must provide reasonable assurances that System institutions will: • **Follow and achieve business plan objectives and policies and procedures requirements regarding E-**	FCA Regulation 609.940.	E-Banking Booklet (Aug. 2003) pp. 21, 26-36. FedLine Booklet (Aug. 2003), p. 13.

E-commerce

Element Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
commerce; and • **Prevent and detect material deficiencies on a timely basis.** ***Reason:*** *A strong internal control system provides the framework for the accomplishment of management objectives, safeguarding of assets, accurate financial reporting, and compliance with laws and regulations. Effective internal controls serve as checks and balances against undesired actions and, as such, provide reasonable assurance that institutions operate in a safe and sound manner. The lack of internal controls puts institutions at risk of mismanagement, waste, fraud, and abuse.*		Management Booklet (Jun. 2004), p. 26.
Electronic Record Retention		
Records stored electronically must be accurate, accessible, and reproducible for later reference. ***Reason:*** *Each System institution may maintain all records electronically, including those recorded originally on paper. The stored electronic record must accurately reflect the information in the original record. The electronic record must be accessible and capable of being reproduced by all persons entitled by law or regulations to review the original record*.	FCA Regulation 609.945.	E-Banking Booklet (Aug. 2003), p. 16.
E-Sign Act		
If using Electronic Signatures: • **Develop policies and procedures to comply with the E-Sign Act.** • **Obtain the customer's agreement to provide electronic disclosures.** • **Confirm the customer's technological capacity to receive required disclosures prior to providing electronic disclosures.** • **Continue paper notification on notices of default, acceleration, repossession, foreclosure, or eviction when secured by the primary residence.** ***Reason:*** *E-Sign preempts (with some exceptions) provisions in most State or Federal statutes or regulations, including the Farm Credit Act of 1971, as amended (Act), and its implementing regulations, that require contracts or other records to be written, signed, or in non-electronic form. With the parties' agreement, institutions can engage in E-commerce in many situations. E-Sign does not, however, allow electronic communications for a*	Electronic Signatures in Global and National Commerce Act (E-Sign)(Pub. L. 106-229).	E-Banking Booklet (Aug. 2003) pp. 5-7, 39.

E-commerce

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
notice of default, acceleration, repossession, foreclosure, eviction, or the right to cure when an individual's primary residence secures the loan. E-Sign also does not apply to writing or signature requirements under the Uniform Commercial Code, other than sections 1-107 and 1-206 and Articles 2 and 2A. E-Sign preempts only those statutes and regulations that relate to business, consumer, or commercial transactions. *Consumers who use electronic signatures should be afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce.*		
Internet Domain Names		
Protect the institution's internet domain name(s) by: • **Registering and renewing domain names in a timely manner** • **Conducting periodic Internet searches for the institution's legal or trade names** ***Reason***: *Timely registration and renewal of domain names are important to ensure that an institution acquires and retains ownership of the Internet address(es) that it desires. Any lapses in registration could result in the loss of a domain name to another party and create customer confusion, reputation harm, fraud, etc.* *Internet searches of institution names may identify other parties attempting to confuse or misdirect customers. Additionally, some web sites have been created to publish harmful information about an organization or to redirect customers by using a domain name similar to that of the original institution.*	FDIC FIL-77-2000, "Protecting Internet Domain Names" (Nov. 8, 2000).	E-Banking Booklet (Aug. 2003) pp. 35.
Authentication of Customers		
Use reliable authentication methods for on-line customer transactions. These methods include the use of passwords, PINs, digital certificates and Public Key Infrastructure, physical devices such as tokens, and biometrics. ***Reason***: *As a customer's business with an FCS institution migrates from paper-based, person-to-person transactions to remote electronic access and transaction initiation, the risk of doing business with unauthorized or incorrectly identified people must*	FCA Informational Memorandum, "Guidance on Authentication in an Electronic Banking Environment" [FFIEC Guidance August 8 2001] (July 2, 2002). ISO/IEC 17799:2000, Section 8.7.6, "Publicly	E-Banking Booklet (Aug. 2003) pp. 7, 30-34.

E-commerce

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
be evaluated. Failure to control this risk by implementing an authentication program could result in both financial loss and reputation damage to an institution. Additionally, effective authentication can help reduce fraud and promote the legal enforceability of electronic agreements and transactions.	Available Systems."	
Insurance Coverage		
Ensure insurance coverage is commensurate with the level of the institution's E-commerce activities and risk appetite. ***Reason:*** *Institutions should have a risk management program in place to manage the risks inherent in their operations. Insurance can play a role in mitigating risks to an acceptable level so the strategic objectives of the institution can be achieved.* *The availability and extent of insurance coverage varies by carrier. Examples of the kinds of risk for which coverage now exists in the marketplace include:* • *Vandalism of institution web sites* • *Attacks against institution systems with the intent to slow or deny service* • *Loss of related income* • *Computer extortion* • *Theft of confidential information* • *Violation of privacy* • *Litigation (breach of contract)* • *Destruction or manipulation of data (including a virus)* • *Fraudulent electronic signatures on loan agreements* • *Fraudulent instructions via e-mail* • *Certain events impacting systems not under the institution's control (e.g., service provider)* • *Insiders who exceed system authorization* • *Actual or threatened situations requiring the use of negotiators, public relation consultants, security consultants, programmers, substitute systems, etc.* *The risks noted above are primarily addressed in optional coverage. It is important for an institution to understand what is specifically covered in existing and prospective insurance policies. Exclusions in coverage may apply in a variety of circumstances.*	FCA Informational Memorandum, "Insurance Considerations for E-commerce Activities" (Dec. 20, 2001).	E-Banking Booklet (Aug. 2003), p. 18. Management Booklet (Jun. 2004), p. 28

E-commerce

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
Weblinking		
Plan, implement, and supervise weblinking arrangements. ***Reason:*** *Customers and visitors to the web site may become confused about the institution's relationship with the third party and its products. An institution's disclosures to customers and visitors to the web site, including the institution's privacy policy, must be clear and concise to avoid confusion. The disclosures must also ensure that customers and visitors to the web site understand that the institution does not endorse or guarantee a third party's products or services. To avoid potential legal risks, an institution must define the rights and responsibilities of a weblinked third party in formal contracts or agreements.*	FCA Informational Memorandums, "Guidance for Weblinking Relationships" (Sept. 19, 2002); "Additional Guidance on the Risks of Weblinking" (June 4, 2003).	E-Banking Booklet (Aug. 2003) pp. 5-6.
Electronic Mail (E-mail) Policy		
Establish a clear policy regarding the use of e-mail that addresses: • **Attacks on e-mail;** • **Protection of e-mail attachments;** • **Guidelines on when not to use e-mail;** • **Expectations that employees will not compromise the company;** • **Use of encryption to protect the confidentiality and integrity of electronic messages;** • **Retention of messages which, if stored, could be discovered in cases of litigation; and** • **Additional controls for examining messages that cannot be authenticated.** ***Reason:*** *E-mail differs from traditional forms of business communications by its speed, message structure, degree of informality, and vulnerability to unauthorized actions. Risks include unauthorized access to data, modification of messages, inaccurate addressing or misdirection, and legal considerations (such as the potential need for proof of origin, delivery, etc.).*	ISO/IEC 17799:2000, Section 8.7.4.2, "Policy on Electronic Mail."	E-Banking Booklet (Aug. 2003) p. 30.
Web Site Content		
Ensure only appropriate content is published on an institution's web site and protect this content from unauthorized alteration.	NIST (National Institute of Standards and Technology) Special Publication 800-44,	E-Banking Booklet (Aug. 2003) pp. 8, 37-39.

E-commerce

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
Reason *Web sites are often one of the first places that malicious entities search for valuable information. Some generally accepted examples of what should not be published on a public web site, or at least should be reviewed carefully before publication, include:* • *Classified or proprietary information;* • *Information on the composition or preparation of hazardous materials or toxins;* • *Sensitive information relating to homeland security;* • *An organization's detailed physical and information security safeguards;* • *Details about an organization's network and information system infrastructure (e.g., address ranges, naming conventions, access numbers);* • *Information that specifies or implies physical security vulnerabilities; and* • *Detailed plans, maps, diagrams, aerial photographs, and architectural drawings of organizational buildings, properties, or installations* *While information on public web sites is intended to be public, assuming a credible review process and policy is in place, it is still important to ensure that information cannot be modified without authorization. Users of this information rely upon the integrity of such information even if the information is not confidential.*	"Securing Public Web Servers."	Management Booklet (Jun. 2004) p. 3
Web Site Compliance		
Ensure the institution's web site contains clear and conspicuous disclosures of the following: • **A privacy statement that identifies the information the web site gathers automatically or collects from e-mails or web forms, how the information is used, how the intrusion detection process may help law enforcement identify harmful intrusions, and a statement on weblinking.** • **A specific statement identifying the institution as an equal credit opportunity lender if the web site contains an online loan or lease application or even advertises credit availability.** • **A specific statement identifying the institution as an equal housing lender if the web site advertises rural residence loans.**	FCA Regulation 626.6020. FCA Informational Memorandums, "Web Site and Internet Guidelines" (Nov. 8, 1999); "Guidance for Electronic Delivery of Disclosures" (Oct. 23, 2001); "Children's Online Privacy Protection Act of 1998" (June 26, 2003);	E-Banking Booklet (Aug. 2003) pp. 37-39.

E-commerce

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
• **A specific statement identifying the institution as an equal opportunity employer if the web site contains job announcements or online job applications.** • **The institution's official name including any parent/subsidiary relationship.** • **If the System institution directs its site or an area of its site to children, it must comply with the Children's Online Privacy Protection Act (COPPA) and have a privacy statement that tells visitors about the types of information the web site collects, how the site collects the information, how the site uses the information, and whether the site gives the information to anyone else. The privacy policy must be clearly written, understandable, and located close to any requests for information from children.** ***Reason***: *Financial institutions need to adapt to a changing technological environment to maintain compliance with laws while using new technologies. For example, the FCA considers every institution's on-line system top-level page, or "home page," to be an advertisement. Therefore, according to FCA regulations, each site should contain the same disclosures as would be appropriate for a paper advertisement.* *FCS institutions should comply with federal laws to provide appropriate disclosures to consumers, protect customer information, and minimize financial liability and reputation risk.* *The privacy of consumer personal information has become an increasing concern with the rapid growth in electronic commerce conducted over the Internet, emerging electronic payment systems, financial services industry consolidation, new business affiliations, and bundling of financial services. Financial institutions are increasingly deploying online systems to facilitate the convenient delivery of services. Some institutions use Internet web sites designed to collect information from consumers via online forms, surveys or e-mail links. Information about consumers is also collected through inconspicuous means such as hidden, undisclosed electronic information collection methods (e.g., "cookies"). Because of this, consumers are increasingly concerned about the collection, use and dissemination of personal information, particularly in the online environment. While consumer concerns about privacy are not uniform, studies have shown that the vast*	"Recommended Elements of a Privacy Policy" (July 29, 2003). FCA Board Policy #78. FFIEC Guidance on Electronic Financial Services and Consumer Compliance (July 15, 1998). FDIC FIL-86-98, "Electronic Commerce and Consumer Privacy" (Aug. 17, 1998). Children's Online Privacy Protection Act (COPPA) 15 U.S.C. §§ 6502-6506.	

E-commerce

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
majority of consumers want the ability to control their personal information and to feel comfortable with how it is used.		